The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

No. 2002-0023-4T

INDEPENDENT STATE AUDITOR'S REPORT ON EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE ARCHITECTURAL ACCESS BOARD

June 1, 2001 through November 16, 2001

OFFICIAL AUDIT REPORT

DECEMBER 19, 2001

TABLE OF CONTENTS

INTRODUCTION

The Architectural Access Board (AAB) is a regulatory agency within the Massachusetts Executive Office of Public Safety. The AAB is mandated to develop and enforce regulations designed to make public buildings accessible, functional, and safe for use by persons with disabilities. The Board consists of nine-members, six of whom are appointed by the Governor in consultation with the Secretary of Public Safety from lists submitted by the Director of the Office on Disability and three are selected by general advocacy groups for persons with disabilities. Two out of the nine Board members are required to be registered architects. The nine-member Board meets every other Monday in order to hear requests for variances by building owners and other individuals responsible for complying with the regulations. In addition, the Board also hears complaints pertaining to buildings that may be in violation of the AAB regulations. The Board is staffed by an Executive Director and three staff members.

The Architectural Access Board's mandated rules and regulations, which appear in the code of Massachusetts Regulations 521 CMR 1:00, have been incorporated into the Massachusetts building code as a "specialized code," making them enforceable by all local and state building inspectors as well as by the Board itself. These regulations are designed to provide full and free access to buildings and facilities for persons with disabilities to enable them to have educational, employment, living, and recreational opportunities necessary to be as self-sufficient as possible and assume full responsibilities as citizens.

At the time of our audit, the primary information technology (IT) functions for AAB were maintained and supported through a file server at the Executive Office of Public Safety. The Board's four microcomputer workstations were connected to the file server. While each Board staff member had access to application software for case tracking, access to MMARS data was limited to the Executive Director and a staff person at the Board of Building Regulations and Standards who provides administrative support. All staff members of the Board have access to File-maker software (case tracking application system for identifying and monitoring complaints and variances) and Microsoft suite.

The Office of the State Auditor's examination was limited to a review of certain IT general controls over and within the AAB's IT environment and controls related to the collection, receipt, and deposit of income.

AUDIT SCOPE, OBJECTIVES AND METHODOLOGY

Audit Scope

From October 29, 2001 to November 16, 2001, we performed an information technology (IT) audit at the Architectural Access Board covering the period of June 1, 2001 to November 16, 2001. Our audit scope included a review of IT-related general controls pertaining to organization and management, physical security, environmental protection, system access security, hardware and software inventory business continuity planning, and on-site and off-site backup. In addition, we reviewed controls related to the collection, receipt, and deposit of income for the monies collected at the time an application is submitted for a variance.

Audit Objectives

We sought to determine whether the Architectural Access Board's (AAB) IT-related internal control environment provided reasonable assurance that control objectives would be met to support business functions. We sought to determine whether IT organizational and management controls were in effect over data processing activities to ensure that such activities are managed effectively and efficiently and that IT policies and procedures are adequately documented. We sought to determine whether adequate physical security and environmental protection were in place over IT resources at the AAB office as well as at the area housing AAB's file server located at the Executive Office of Public Safety (EOPS).

We sought to determine whether adequate controls were in place to prevent unauthorized system access to the data files and software residing on the Board's microcomputer workstations and file server. Our objective with respect to the Board's hardware and software products was to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-resources were properly accounted for in an inventory record and safeguarded against unauthorized use, theft, or damage.

Regarding system availability, we determined whether controls were in place to provide reasonable assurance, through a business continuity plan, that required IT processing and access to data files could be regained within an acceptable period of time should IT systems be rendered inoperable or inaccessible and whether adequate on-site and off-site storage of backup media was in effect to assist recovery efforts.

We also sought to determine whether cash receipts and deposits were properly recorded and whether deposits were made in a timely manner as determined through a review of bank statements.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations and reviewing documentation regarding AAB's mission, operations, and IT organization and management. We interviewed the Board's Executive Director and IT staff from the Executive Office of Public Safety to obtain an understanding of the Board's operations and information technology control environment. In conjunction with our review of the internal control environment, we evaluated the degree to which the Board had documented, authorized, and approved IT-related internal control policies and procedures for maintaining and monitoring cases through its case tracking system.

To accomplish a preliminary review of the adequacy of general controls over IT-related functions and assets, we obtained an understanding of and observed computer systems at the Board's office. We also conducted a site visit to the area housing the Board's file server at the EOPS's office. To assess the adequacy of IT general controls, we interviewed AAB staff, observed operations, and performed selected audit tests.

Regarding our review of IT organization and management, we interviewed the Executive Director, requested documented IT policies and procedures and reviewed operational procedures, and analyzed relevant documentation. To determine whether IT-related assets, including the file server and microcomputer-based data files and software at the Board's office and at the EOPS office, were adequately safeguarded from damage or loss, we reviewed physical security and environmental protection over IT resources through observation and interviews with the Board's and EOPS staff.

To assess the adequacy of controls to provide continued operations, we assessed the degree to which business continuity plans were required for the Board and whether steps had been taken to implement recovery and contingency plans to regain important operations should IT systems be rendered inoperable. In addition, we interviewed the Board's staff to determine whether a written, tested business continuity plan was in place, whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. Further, we assessed the degree to which copies of backup computer media were stored in secure on-site and off-site locations through interviews with the Board and EOPS staff.

Our examination of system access security controls included a review of access privileges of those employees authorized to access automated systems. To determine whether existing system-based access privileges were authorized and reflected current responsibilities, we reviewed procedures for granting and updating system access. To determine whether access security was being properly maintained through the management of user-IDs and passwords, we interviewed the Board's staff and assessed the level of access security being provided. We determined whether procedures were in place to ensure that the EOPS was promptly and properly notified when a change in personnel status (e.g., employment termination, job transfer, or leave of absence) occurred so that the user-ID and password could be promptly deactivated from the system or the access privileges appropriately modified.

We conducted interviews and reviewed control documentation from the Board to determine the adequacy of hardware and software inventory control policies and procedures. We obtained and reviewed an IT-related asset inventory record, which included four microcomputers workstations and software products to support the Board's operations. To determine whether the Board's hardware inventory records were current, accurate, and valid, we compared all computer hardware inventory items appearing on the computer hardware inventory listing to the actual computer hardware on hand. We performed a test of the inventory record, tracing all of items from the list to the floor. To determine whether inventory records were current, accurate, and valid, we performed a test of items listed on the inventory list and compared them to their physical locations. We evaluated the adequacy of inventory controls through tests and observations by assessing the integrity of the inventory record, determining whether computer hardware was properly tagged and in good condition, and whether the Board conducted an annual physical inventory of fixed assets and reconciliation to the inventory record. We also determined whether adequate controls were in place to provide reasonable assurance that microcomputer based software would be properly accounted for by reviewing the inventory record.

To determine whether adequate internal controls were in place regarding the Board's receipt, deposit and reconciliation of income, we interviewed the Executive Director and obtained and reviewed relevant procedures and documentation, including bank statements and the subsidiary cash receipt ledger. Using Board-supplied information and discussions with staff, we evaluated the monitoring procedures used to monitor the timeliness of cash receipt deposits.

Our review was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and industry auditing practices. The audit criteria used for our control examination were based on applicable legal requirements and generally accepted IT control practices.

AUDIT SUMMARY

Based on our examination, we determined that controls in place provided reasonable assurance that control objectives pertaining to IT-related physical security, system access security, environmental protection, and on-site backup of computer media would be met. With respect to selected administrative control areas, our review indicated that the Board had in place a case tracking system to manage its ongoing complaint and variance investigation cases. However, our audit revealed that controls needed to be strengthened with regard to the documentation of IT policies and procedures and the timely deposit of cash receipts.

Our review of IT-related organization and management disclosed that certain organizational controls were in place considering the inherent control weaknesses associated with a very small entity. Although certain operational procedures were not formally documented, staff were knowledgeable with respect to their responsibilities. Regarding IT-related functions, such as access security, physical security over IT resources, and business continuity planning, there was little documentation of the policies and procedures that governed actions taken with respect to authorized access to systems, physical security and environmental protection, hardware and software inventory control, and decisions regarding the extent to which recovery and contingency should be in place. With respect to the latter, we acknowledge management's position as to the level of criticality of the automated systems that the Board uses and that operations could still be performed.

We found that internal controls in place provided reasonable assurance of adequate physical security and environmental protection of the Board's four workstations at the central office location and the file server at the Executive Office of Public Safety. With respect to physical security, personnel entering the building facility are subject to building security controls, and the office area is located in a protected area and would be staffed when open. We found that the Board's office and the EOPS's file server room are located in securely locked areas. Our audit also revealed that there were adequate environmental protection controls in place and operating, including fire-suppression devices and smoke detectors to protect IT-related assets.

We found that the Board did not have a formal business continuity strategy and plan to help ensure resumption of mission-critical and essential processing within an acceptable time frame should processing be rendered inoperable or inaccessible. Although the risk to continued operations is relatively low should IT systems be rendered inoperable, we suggest that the Board assess the adequacy of EOPS recovery plans and develop contingency plans, if needed, to the degree required to avoid operational difficulties and unnecessary data or system reconstruction costs. In addition, although procedures were in effect for on-site storage of backup media for the file server, it appeared that the EOPS was not backing the Board’s file server off-site. Understandably, the provision of off-site storage of backup copies of magnetic media would further ensure system availability. We suggest that the Board determine the viability of the EOPS’s recovery and business continuity plans and to assess, in conjunction with EOPS, the criticality of the Board’s automated systems and review and test any recovery plans developed on behalf of the Board. Backup copies of computer media are generated by EOPS since they have custodial and operational responsibility of the file server supporting the Board’s operations. Because the frequency of on-site backup is on a weekly basis, and no off-site storage of backup media is provided, the Board should review provisions for available backup media to ensure that adequate resources for recovery would be available.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized users had access to the Board’s data files and programs residing on computer and application systems. We found that administrative controls over user-IDs and passwords provided reasonable assurance that access privileges would be deactivated or appropriately modified should the Board’s employees terminate employment or incur a change in job requirements. During the course of our audit, nothing came to our attention to indicate that there were weaknesses in access security to the Board’s case tracking system.

With respect to hardware and software inventory control, we found that the Board, although not maintaining documented policies and procedures, did have an inventory record delineating all of its hardware and software products. The inventory control procedures provided reasonable assurance that all IT-related assets were adequately listed, identified, and controlled, and our review of inventory items located in the Board’s office indicated that all of the items were locatable and properly accounted for. Although we noted that all items could be located, were in good condition, and were being utilized, we recommend that the Board, in conjunction with EOPS, formalize procedures for tagging all the Board’s IT equipment and conduct an annual physical inventory to validate information on the inventory list. We found appropriate controls in place regarding the maintenance of the inventory record for software products and licenses and the use of only authorized software.

Our review of internal controls regarding the Board’s receipt, deposit, and reconciliation of income revealed that relevant procedures and documentation, including bank statements and subsidiary cash receipt ledger, did exist and were properly maintained. However using Board-supplied information and through discussions with the Board’s staff, we determined the monitoring procedures used by the Board to ensure the timeliness of cash receipt deposits needed to be strengthened. We recommend the Board either initiate daily deposits or seek a waiver from requiring the daily deposit of all cash receipts.

AUDIT RESULTS

IT-related Organization and Management

Although our audit revealed that the AAB had certain IT-related general controls in place, control practices needed to be strengthened by having IT-related policies and procedures formally documented to provide sufficient guidance for performing IT-related functions and operations. Because IT operations are limited and are supported by office-based systems, the extent of required documentation for IT-related functions is not extensive. We acknowledge the Board's difficulty in allocating resources to document IT-related procedures. We believe, however, that overall control practices would be strengthened by documenting policies and procedures regarding access security, physical security, hardware and software inventory control, and, if required, business continuity planning. Documented procedures might also cover information technology planning, risk assessment and risk management, definition of information architectures, data management for the case tracking system, virus protection, authorized use of IT resources, training, and monitoring and reporting. Although certain control practices and procedures were being performed with regard to some of these functions, written policies and procedures would help ensure that important operational and control objectives would be met. Documentation could also be extended to decisions regarding disaster recovery requirements and contingency plans.

Formal documentation of IT-related policies and procedures provides a sound basis for helping to ensure that desired actions are taken and that undesired events are prevented or detected and, if detected, that corrective action is taken in a timely manner. Documented policies and procedures also assist management in training staff and serve as a good basis for evaluation. They also enhance communication among personnel to improve operating effectiveness and efficiency. Clearly, formal documentation enables trained personnel to develop a broader understanding of their duties and improve their levels of competence.

In the absence of formal standards, policies, and procedures, employees may rely on individual interpretations of what is required to be performed or how to best control IT-related systems and resources. In such circumstances, inconsistencies or omissions may result and key control objectives may not be adequately addressed. In addition, management may not be adequately assured that desired actions will be taken. Furthermore, the absence of documented policies and procedures undermines the ability to monitor and evaluate IT operations and application systems because of the absence of stated internal controls and required audit or management trails. In addition to being a generally accepted control practice, Massachusetts General Laws, Chapter 647, requires that all state agencies have documented and approved internal control procedures.

Recommendation:

We recommend that the Architectural Access Board begin documenting its IT-related policies and procedures to provide sufficient formal guidance to IT operations. Also, AAB should develop and implement a formal business continuity strategy and plan to help ensure system availability and resumption of IT operations within an acceptable time frame should processing be rendered inoperable or inaccessible.

Auditee's Response:

> *As you are aware, the current staff of the Board consists of 4 people. However, one staff person is currently on extended sick leave and another has been out due to surgery. Therefore, the staff has been cut in half and our ability to carry out our mission has been extremely difficult.*
>
> *However, let me assure you that we will seeking a waiver from the requirement of daily deposits of all cash receipts to allow the agency to deposit weekly. Given the small amount of deposits in any given week, daily deposits seem an unnecessary burden for an agency of this. We will also begin to develop an IT control policy and procedure manual in the event that the agency has a change in staff in the future.*

Auditor's Reply:

We recognize the Board's staff limitations to initiate additional tasks. We believe the process can be initiated by first documenting a framework for IT-related policies and procedures and incorporating good practices for IT security promoted by the Commonwealth's information technology division and the CobiT control model. We agree with your efforts to seek a waiver for deposit of cash receipts. Documented controls are even more important to institute to assure compliance with managements business objectives for newly hired staff to become familiar with IT control policies and procedures.